

Debunking the Myths of Disk Encryption

Addressing Common Myths

July 2010



Debunking the Myths of Disk Encryption

Disk encryption is rapidly becoming one of the must-have forms of security for today's business computers. However, some organizations who could benefit greatly avoid taking advantage of this fundamental form of data protection. Today's centrally-managed disk encryption packages provide one of the easiest and most practical methods of protecting data that is stored, processed or transmitted electronically. It's time to take another look at some of the misconceptions about encryption.

Myth: Most of my PC's don't have anything worth stealing on them

Many laptops are stolen for the hardware itself, just as much as for any data that might be on them. In addition, privacy regulations keep getting stricter – what's okay today will very likely not be next year. In fact, in some places, losing control of something as simple as a list of email addresses and names can put your business in violation. Most compliance requirements now require encryption of all data, especially when it's on disk.

Myth: Users won't use disk encryption, it's too difficult

Disk encryption is easy to install and works automatically behind the scenes. Users only see it when they boot up their computer—and then all they have to do is type their Windows password or just touch a fingerprint reader. There's nothing to remember when using the PC and nothing special to do when shutting down.

Myth: Disk Encryption makes PCs too slow to use

Most users will not notice the difference other than when they first log in to their computer and see the encryption log in screen. Encryption does slightly slow down the start up and shut down process, but the difference is measured in seconds. According to Forrester Research, the impact on system performance is less than 5%.

Myth: Users will simply disable disk encryption

This can be true of unmanaged disk encryption products. For example, more than half of the U.S. business managers in a recent Ponemon Institute study reported disabling individually set up laptop encryption, making data on those computers vulnerable. (Similar results occurred in Canada and the United Kingdom.) However, centrally-managed disk encryption packages typically enable the administrator to prevent users from turning off disk encryption. Such packages give your business the ability to ensure that data remains protected.



Myth: Forgotten passwords will cause more lockouts and make the whole PC worthless

Be sure your encryption solution provides emergency access recovery so that Administrators create a special “one-time” password to unlock the user’s PC. This protects you so that forgotten passwords or departing employees can’t cause valuable data to be lost.

Myth: Disk encryption software is expensive

Disk encryption software has come a long way since it was first launched and pricing has come down considerably. To save money, look for a complete security suite package that combines disk encryption with other security applications. This makes disk encryption more affordable and gives you even higher security as well.

Myth: Physical security is enough

Some facilities are built like Fort Knox. Other organizations may only be one shattered window away from having computer equipment stolen. Notebook computers are often taken home at night. How secure are their homes? There are many stories of folks who have had their notebook removed from their car or from their chair at a restaurant.

According to the Ponemon Institute, over 12,000 notebook computers are lost in airports each week with 70% never being reclaimed. When physical security fails, encryption provides another layer of protection.



Myth: Only major corporations need encryption

With data breach notification laws requiring written notification to customers when their data has been stolen or lost, any size organization can face potential liability and subsequent losses. The Ponemon Institute reports that the average costs of a data breach runs around \$204 per each record lost. These costs include notification, credit monitoring services, investigations and loss in business. Disk encryption software is an inexpensive insurance policy and can prevent many public data breaches.

Make Disk Encryption Simple with DigitalPersona® Pro

Of course, the best way to dispel the encryption myths is to test encryption yourself. Encryption should not be solely relied on for security, but should be part of an entire package of centrally managed protection.

DigitalPersona Pro encryption software is available for test drives and is part of a complete endpoint security protection package that often costs less than most companies charge for encryption software by itself. Go to <http://www.digitalpersona.com/diskencryption> to get your free download of DigitalPersona Pro.

© 2010 DigitalPersona Inc. All rights reserved. DigitalPersona is a trademark of DigitalPersona, Inc., registered in the United States and other countries. All other trademarks referenced herein are the property of their respective owners.